



## INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

PIPEDRIVE CRM PLATFORM

FOR THE PERIOD OF OCTOBER 1, 2022, TO SEPTEMBER 30, 2023

Attestation and Compliance Services



**Proprietary & Confidential**

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

## INDEPENDENT SERVICE AUDITOR'S REPORT

To Pipedrive Inc.:

### Scope

We have examined Pipedrive Inc.'s ("Pipedrive") accompanying assertion titled "Assertion of Pipedrive Inc. Service Organization Management" ("assertion") that the controls within Pipedrive's Pipedrive CRM Platform system ("system") were effective throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Pipedrive's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Pipedrive uses various subservice organizations for cloud hosting and managed database services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Pipedrive, to achieve Pipedrive's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

### Service Organization's Responsibilities

Pipedrive is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Pipedrive's service commitments and system requirements were achieved. Pipedrive has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Pipedrive is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

### Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Pipedrive's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Pipedrive's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

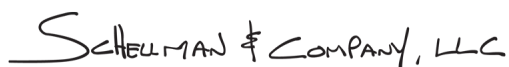
### *Inherent Limitations*

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that Pipedrive's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

### *Opinion*

In our opinion, management's assertion that the controls within Pipedrive's Pipedrive CRM Platform system were effective throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Pipedrive's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

SCHEELMAN & COMPANY, LLC

Washington, District of Columbia  
November 27, 2023

## ASSERTION OF PIPEDRIVE SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Pipedrive Inc.'s ("Pipedrive") Pipedrive CRM Platform system ("system") throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Pipedrive's service commitments and system requirements relevant to security, availability, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Pipedrive's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Pipedrive's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2022, to September 30, 2023, to provide reasonable assurance that Pipedrive's service commitments and systems requirements were achieved based on the applicable trust services criteria.

# DESCRIPTION OF THE BOUNDARIES OF THE PIPEDRIVE CRM PLATFORM SYSTEM

## Company Background

Pipedrive is a software development company that implements customer relationship management (CRM) software for enterprise clients. The Pipedrive software is utilized by over 100,000 companies around the world. Pipedrive is most widely used as a CRM program to drive sales and grow the bottom line, but it has also been used in other facets. Pipedrive was founded in Tallinn, Estonia in 2010 and has since expanded to Tartu Estonia, Lisbon Portugal, London England, Dublin Ireland, Riga Latvia, Berlin Germany, Prague Czech Republic , Florida and New York, United States.

The Sales Management System software as a service (SaaS) product was developed with activity-based selling in mind. Activity-based selling is a sales management strategy that links the cause-and-effect relationship between sales activities and business results.

## Description of Services Provided

The Pipedrive CRM Platform is a web-based sales CRM and pipeline management solution that enables businesses to plan their sales activities and monitor deals. Pipedrive streamlines actions involved in converting a potential deal into a sale. As a cloud-based application, the solution can be accessed from anywhere 24x7 using a web browser or dedicated mobile apps.

Pipedrive provides sales personnel visibility of different sales pipelines. An interface displays the progress stages for each deal with the complete details for next actionable items. The activity & goal feature allows users to track the pending activities in each pipeline. Pipedrive also offers custom sales reporting tools to monitor individual and team level targets, analyze sales data and generate visual reports.

Pipedrive's mailing system integrates with multiple e-mail service providers. Users can send and receive e-mails from multiple accounts using their Pipedrive account. The solution also integrates with various leading CRM tools to transfer contact details, communication history and other information across applications.

## System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

## Principal Service Commitments and System Requirements

Pipedrive designs its processes and procedures related to its Pipedrive CRM Platform system to meet its objectives. Those objectives are based on the service commitments that Pipedrive makes to user entities, the laws and regulations that govern SaaS providers, and the financial, operational, and compliance requirements that Pipedrive has established for the services. The Pipedrive CRM Platform services of Pipedrive are subject to the General Data Protection Regulation (GDPR) regulations and state privacy and security laws and regulations, such as the California Consumer Privacy Act, in the jurisdictions in which Pipedrive operates.

Security, availability, confidentiality, and privacy commitments are documented and communicated in service level agreements, standardized contracts, and policies and procedures. The principal security, availability, confidentiality, and privacy commitments are standardized and include, but are not limited to, the following:

- Security – Pipedrive sets security principles within the fundamental designs of the Pipedrive CRM Platform system that are designed to permit system users to access the information they need based on the

permission of least privileged provisioning. Pipedrive is committed to the use of encryption protocols to protect customer data at rest and in transit.

- Availability – Pipedrive manages capacity demands through the monitoring and evaluation of current processing capacity and usage rates. Pipedrive meets company objectives through authorization, design, development, and monitoring of data backup processes and recovery infrastructure.
- Confidentiality – Information is defined and classified into categories with associated retention periods. Pipedrive maintains data retention policies and procedures to guide personnel in performing data retention and disposal activities. Pipedrive follows generally accepted industry standards to protect the information submitted, both during transmission and upon receipt. Pipedrive will store data on behalf of the client until the termination of Pipedrive services. Upon termination, Pipedrive will store the client's data as described in Pipedrive Privacy notice <https://www.pipedrive.com/en/privacy#data-retention>.
- Privacy – Pipedrive is committed to documenting privacy notices that include provisions for collection, use, disclosure, and disposal of personal information. Pipedrive retains the personal data collected from a user for as long as the user's account is active or otherwise for a limited period of time as long as it's needed it to fulfill the purposes for which they have initially collected it, unless otherwise required by law.

Pipedrive Privacy Notice covers the collection and use of information obtained through the Pipedrive CRM Platform and through their use of Pipedrive services. Pipedrive Privacy Notice covers the collection and use of information obtained through the Pipedrive CRM Platform through their use of Pipedrive services. For additional commitments related to privacy, please see the below listing of PNCs (Privacy Notice Commitments):

- Pipedrive works with third-party service providers who provide website, application development, hosting, maintenance, and other services. Pipedrive limits the information provided to these service providers to that which is reasonably necessary for them to perform their functions, and Pipedrive contracts and requires them to maintain the confidentiality of such information.
- In the event of a security systems breach, Pipedrive will inform customers and the authorities of the occurrence of the breach in accordance with applicable law.
- Pipedrive has no direct relationship with the client's customers or third party whose personal data it may process on behalf of a client. An individual who seeks access, or who seeks to correct, amend, delete inaccurate data, or withdraw consent for further contact should direct his or her query to the client or user they deal with directly.
- Pipedrive implements appropriate administrative, technical & physical safeguards to prevent unauthorized access, use, modification, disclosure, or destruction of the information entrusted to them. These measures have been audited and certified to industry standards.
- Pipedrive's use of information received and Pipedrive's transfer of information to any other app from Google APIs will adhere to Google API Services User Data Policy, including the Limited Use requirements.

Pipedrive establishes operational requirements that support the achievement of security, availability, confidentiality, and privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Pipedrive's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operation procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Pipedrive CRM Platform system.

In accordance with Pipedrive's assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

## Infrastructure

The Pipedrive CRM environment is supported by infrastructure hosted within Rackspace and Amazon Web Services (AWS). Pipedrive operates under a shared responsibility model with AWS and Rackspace. AWS and Rackspace are responsible for configuring, managing, and monitoring the security of underlying cloud infrastructure (i.e., geographical regions, availability zones, edge locations, components from the host operating system, and virtualization layer and storage). Additional responsibilities for AWS and Rackspace include providing physical safeguarding of IT infrastructure, as well as providing environmental safeguards (e.g., power supply, temperature control, fire suppression, etc.).

The Pipedrive CRM Platform application is written in PHP, NodeJS, and GoLang that runs on multiple Linux servers within Rackspace and AWS. Pipedrive utilizes a cloud load balancer that distributes traffic to application servers running the Pipedrive CRM application which is used to run various scheduled jobs. Backups are stored within AWS.

## People

People and functions involved in the operation and use of the system are:

- Executive Management – responsible for providing execution of business objectives and strategic direction.
- Infrastructure - responsible for building, securing, and maintaining Pipedrive's infrastructure, the team also provides technical expertise on the infrastructure platform and its sub-components hosting the Pipedrive application, its ancillary components, and the necessary tools for day-to-day operations.
- Data Engineering - responsible for database design, construction, and maintenance, ensuring data integrity, availability, and usability, as well as managing user account access and database deployments. This is inclusive of the data management team.
- IT Operations (ITops) – responsible for providing secure workstations and corporate network access used to access the Sales Management System.
- Information/Cyber Security - responsible for conducting risk assessments, managing incidents, raising information security awareness through training, and analyzing vendors' security. Cyber Security team oversee Pipedrive's platform, application, and cloud security, along with vulnerability management. Additionally, the information security department handles business continuity planning and disaster recovery testing.
- HR – responsible for conducting background and security checks on Pipedrive personnel prior to employment. HR provides a mandatory orientation program to employees that stresses the confidentiality of customer information through the new-employee orientation program they deliver.
- Finance and Legal – responsible for Pipedrive's contract management, including service billing and assisting in various controls related to privacy related activities.

## Procedures

### *HR and Training*

Job descriptions are documented and utilized to outline the required skills needed and employee responsibilities for the job. As part of the hiring process, employment candidates are interviewed for the required skillset of the job position the employment candidate is applying for. This includes a resume review, proficiency evaluation, and proof of identity. Upon hire, employees are required to formally acknowledge the employment handbook, that includes confidentiality requirements, as part of the onboarding process. Additionally, an employee non-compliance procedure is documented within the information security policy communicating that an employee may be terminated for non-compliance with a policy and / or procedure.

New hires are required upon hire, and existing employees on at least an annual basis, to complete security awareness training to understand their obligations and responsibilities to comply with the corporate and business

unit security policies. Ongoing training is also provided and available for employees to maintain and further develop their proficiency.

#### *Access, Authentication, and Authorization*

Documented access control policies and procedures are in place to guide personnel in information security practices including access provisioning, password requirements, and access revocation. Access to the organization's production systems is controlled using a single sign on (SSO), which enforces minimum password requirements and multifactor authentication (MFA). Within each layer of the production environment mentioned above, administrator access is restricted to authorized personnel.

#### *Access Requests and Access Revocation*

Upon hire, Pipedrive's HR team initiates a new hire request and checklist within the HR system to document responsibilities and onboarding tasks required by HR and the ITops team. Requests for elevated access are required to be approved by management, which are documented within tickets. User access reviews, including privileged users, are performed by management on an annual and semi-annual basis to help ensure that access to data is restricted and authorized.

When a user leaves Pipedrive, ITops completes a termination ticket and revokes system access rights as a component of the employee termination process. If the access is for asset that is under Okta, the revoke is done automatically. ITops teams are notified of employee termination upon entry of a termination date within the HR system, and a ticket is created to track the access revocation process.

#### *System Security and Monitoring*

Documented information security policies and procedures are in place to guide personnel in system and network security practices. Security and availability logging and monitoring tools are in place to monitor the production network for attempted or actual network breaches and is configured to alert IT security personnel based on predefined alerting thresholds and expected user behavior and system activity. Upon the triggering of an alert, on-call security operations center personnel triage potential incidents utilizing the internal incident management system.

Pipedrive monitors production systems through daily business operations as well as separate assessments that occur periodically throughout the year. Continuous system monitoring of the production environment and company assets is performed utilizing various tools for security threat monitoring, infrastructure monitoring, and network malicious activity monitoring.

Additionally, management monitors the security impact of emerging technologies and threats and the impact of applicable laws or regulations for the Pipedrive services. This helps ensure continued system security and compliance with regulatory requirements and commitments made to customers.

#### *Incident Response*

Documented incident management policies and procedures are in place for identifying, documenting, escalating, resolving, and determining lessons learned for failures, incidents, concerns, and other complaints. These policies and procedures outline the key steps through an incident lifecycle, including lessons learned and considerations to prevent incident recurrence. In addition to the incident management policy and procedures established for internal users, an external support customer portal has also been established to provide external users a method of communication to report incidents.

#### *Data Backup, Replication, and Disaster Recovery*

Pipedrive has established a formal set of policies and procedures to help guide personnel in data backups. Pipedrive utilizes backup systems to perform automated backups of production systems. The backup systems are also configured to send e-mail notifications and slack alerts to ITops personnel regarding backup job completion status. If a backup job fails, Infrastructure team will investigate and resolve the failure as required. The database backup system is configured to encrypt backups. In addition to backups, Pipedrive utilizes replication and redundant architecture to help protect against the loss of data. Automated monitoring and alerting is set up replication status of backups and system uptime on an ongoing basis.



Backup recovery tests are performed quarterly for selected region to help ensure availability and access to data. In addition to that, the Data Warehouse team is using the backups for selected data on a daily basis. Additionally, disaster recovery procedures are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. In case of a disaster in a production region, Pipedrive can initiate a recovery procedure for that region to be restored into a pre-prepared, designated separate AWS region. The Infrastructure team performs a disaster recovery test on a quarterly basis.

*Change Management*

Change management policies and procedures are in place to guide personnel in the request, documentation, testing, and approval of application and infrastructure changes. A ticketing system is in place to centrally document, manage, and monitor application and infrastructure changes from change request through implementation.

Change management personnel meet on a regular basis to discuss, review, prioritize, and schedule production changes. The security and privacy teams have placeholder time available at least weekly and meet to discuss the current status of change management activities. Topics of the meetings include a roadmap discussion for future changes, discussion / review of changes and releases in development, as well as a review and assessment of recent changes that were deployed to production.

*Vendor Management*

To address risks associated with vendors and vendor oversight, management maintains a vendor review policy and process document for managing risk during vendor contracting and ongoing due diligence procedures. Depending on the vendor and type of services being contracted, various reviews are required that include, but are not limited to, finance, legal, privacy, and security reviews.

*Privacy Notice:*

The privacy notice (“policy”) describes the information that Pipedrive gathers on or through the service, the use and disclose of such information, and the steps taken to protect such information. By visiting the site, or by purchasing or using the service, users accept the privacy practices described in the policy.

This policy is incorporated into, and is subject to, the Pipedrive terms of service. Capitalized terms used but not defined in this policy have the meaning given to them in the Pipedrive terms of service. The Pipedrive privacy notice is available in its entirety on the Pipedrive public website.

Documented policies and procedures are in place to guide personnel of privacy practices for the collection and use of information obtained through Pipedrive CRM Platform and to guide personnel in identifying and managing privacy related risks. These methods are reviewed by company’s management, the data protection officer (DPO), and legal counsel on at least an annual basis.

**Data**

The following table describes the information used and supported by the system:

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Client Data	<ul style="list-style-type: none"><li>Client data uploaded to Pipedrive CRM Platform</li><li>Backups of clients’ data</li></ul>	Secret

**Subservice Organizations**

The cloud hosting services provided by AWS and the managed database services provided by Rackspace were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS and Rackspace, alone or in combination with controls at Pipedrive, and the types of controls expected to be implemented at AWS and Rackspace to achieve Pipedrive's principal service commitments and system requirements based on the applicable trust services criteria.

Control Activities Expected to be Implemented by AWS and Rackspace	Applicable Trust Services Criteria
AWS and Rackspace are responsible for managing and monitoring logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the Pipedrive systems reside.	CC6.1, CC6.2, CC6.3, CC6.5 CC6.6, CC7.1, CC7.2
AWS and Rackspace are responsible for ensuring controls for restricting physical access to data center facilities, backup media, and other system components including network devices, virtualization, and storage infrastructure.	CC6.4, CC6.5, CC7.2
AWS and Rackspace are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where Pipedrive systems reside.	CC6.7
AWS and Rackspace are responsible for ensuring the data center facilities are equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2

Pipedrive has not delegated any responsibility of the personal information life cycle to AWS or Rackspace.

### Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

### Trust Services Criteria Not Applicable to the In-Scope System

The Trust Services criteria presented below, are not applicable to the Pipedrive CRM Platform system within the scope of this examination. As a result, an associated control is not required to be in place at the service organization for the omitted applicable trust services criteria. The following table presents the trust services criteria that are not applicable for the Pipedrive CRM Platform system at Pipedrive. However, Pipedrive will assist the data controller (Pipedrive's customers) in responding to a consumer request.

Criteria #	Reason for Omitted Criteria
P1.1	Providing notice to data subjects is the responsibility of the data controller and not Pipedrive given its role as a data processor.
P2.1	Providing choice to data subjects and obtaining consent is the responsibility of the data controller and not Pipedrive given its role as a data processor.
P3.2	Requiring explicit consent from data subjects is the responsibility of the data controller and not Pipedrive given its role as a data processor.
P5.1	Providing access to data subjects is the responsibility of the data controller and not Pipedrive given its role as a data processor.
P5.2	Correcting, amending, or appending personal information is the responsibility of the data controller and not Pipedrive given its role as a data processor.
P6.1	Obtaining consent from data subjects for purposes of third-party disclosure is the responsibility of the controller and not Pipedrive given its role as a data processor.

Criteria #	Reason for Omitted Criteria
P6.7	Providing an accounting of the personal information held and disclosing a data subject's personal information is the responsibility of the data controller and not Pipedrive given its role as a data processor.